

ORIGINAL

EDOK - Search Warrant (Revised 5/13)

United States District Court

EASTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF:
Information associated with **tstyles77@gmail.com**
and **tstyles77@icloud.com** that is stored at
premises controlled by Apple Inc.

Case No. 23-MJ-34-JAR

SEARCH AND SEIZURE WARRANT

TO: ANY AUTHORIZED LAW ENFORCEMENT OFFICER

An application by a federal law enforcement office or an attorney for the government request the search of the following person or property located in the EASTERN District of OKLAHOMA (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT "A"

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

SEE ATTACHMENT "B"

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE HEREBY COMMANDED to execute this warrant on or before 3/02/2023
(not to exceed 14 days)

- ☐ in the daytime 6:00 a.m. to 10:00 p.m.
☒ at anytime in the day or night as I find reasonable cause has been established

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Jason A. Robertson.

- ☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer after executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check):
☐ for _____ days (not to exceed 30).
☐ until, the facts justifying, the later specific date of _____

Date and time issued: February 16, 2023

City and state: Muskogee, Oklahoma



A handwritten signature in black ink, appearing to read "Jason A. Robertson", is written over a horizontal line.

Judge's signature


JASON A. ROBERTSON
UNITED STATES MAGISTRATE JUDGE
Printed name and title

FILED

APR 11 2023

EDOK - Search Warrant PAGE 2

BONNIE HACKLER
Clerk, U.S. District Court

RETURN		
		By <u> </u> Deputy Clerk
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
23-MJ-34-JAR	2/17/23 @ 3:00 PM	Apple, Inc.
Inventory made in the presence of:		
Inventory of the property taken and name of any person(s) seized:		
electronic contents of Apple accounts associated with tstyles77@gmail.com & tstyles77@icloud.com.		
CERTIFICATION		
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.		
Date: <u>4/6/23</u>	 Executing officer's signature	
	<u>Jordan Siri, Special Agent</u> Printed name and title	

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **tstyles77@gmail.com** and **tstyles77@icloud.com** that is stored at premises controlled by Apple Inc. ("Apple" or "Provider"), headquartered at 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by the provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account(s) listed in Attachment A for the time period of December 1, 2020, until service of the Search Warrant:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile

Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and

all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 7 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2251(e), 2252(a)(4), and/or 2252(b)(2), those violations involving Travis Gene SLOAT and occurring after November 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Discussions regarding SLOAT's attempted surreptitious recording of J.C. or any other minor;
 - (b) Evidence regarding SLOAT's attempts to delete or otherwise conceal attempted surreptitious recordings;
 - (c) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
 - (d) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
 - (e) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
-